As a Security Engineer for Information Technology (IT), you will implement, operate, and maintain technologies that support the Airports Authority's Information Security Program.

JOB PROFILE SUMMARY

- Security Engineer IT
- This is a non-career term job.
- Works under the general supervision of the Chief Information Security Officer.
- Serves in the Information Security Department of the Office of Technology at the Headquarters Office.

Monitors, tests, and reports on the confidentiality, integrity, and availability of information assets in compliance with Airports Authority information security policies and other security and compliance standards. Performs related functions.

GENERAL RESPONSIBILITIES

- Maintains, upgrades, and implements new information security tools.
- Works with other IT staff to ensure appropriate configuration of devices and applications added to Airports Authority networks meet security standards, policies, and regulations.
- Manages and maintains Security Information and Event Management (SIEM) systems to provide real-time monitoring, correlation of security events, notifications, reporting, and development of dashboards.
- Manages and maintains the intrusion prevention systems (IPS), responds to and resolves security alerts, and escalates high risk events to the appropriate team for resolution.
- Reviews firewalls to ensure adequacy of rules for data and systems; ensures review and approval of firewall changes by the Information Security Director prior to their deployment.
- Conducts continuous vulnerability scans and penetration testing on all networks; participates in patch management processes and recommends changes and improvements, as needed.
- Works with other Information Security staff to ensure Payment Card Industry (PCI) regulated environments are continuously compliant with Data Security Standards (PCI-DSS); conducts network and systems audits, end-point assessments and prepares assessment reports.
- Continuously monitors user access to ensure access is authorized, provisioned, and de-provisioned according to policy. Identifies violations and takes measures to resolve and prevent reoccurrence.
- Serves as a primary member on the Security Incident Response Team (SIRT) to respond to, prevent reoccurrence, and recover from security breaches.
- Keeps abreast of security industry developments to proactively identify threats against networks and systems and takes actions to mitigate information security threats.
- Ensures that security architecture standards align with evolving legal and mandated compliance standards.
- Conducts information security awareness training and supports development of newsletters to educate staff and other users on securing networks, systems, and data. Evaluates effectiveness by conducting period phishing tests.
- Performs other duties as assigned.

QUALIFICATIONS

- Five years of progressively responsible experience in Information Security including implementing, upgrading, and maintaining security tools and configuring or reviewing firewalls and conducting security assessments.
- Three of the five years of experience must include implementing intrusion prevention/ detection systems (IPS/IDS), web security tools, e-mail security tools, firewalls, and two-factor authentication devices.

KNOWLEDGE, SKILLS AND ABILITIES (KSAs)

1. Comprehensive knowledge of network and application firewalls, SIEMs, VPNs, and IPS and ability to use at least three of the following technologies: SPLUNK, Tripwire Enterprise, Cisco ASA firewall, Palo Alto firewalls, Sourcefire IPS, or Websense.
2. Knowledge of and skill in implementing, configuring, and fine tuning information security devices to protect organizational systems and networks from security incidents.
3. Comprehensive knowledge of SIRT procedures and skill in detecting, responding to, and analyzing security events and alerts.
4. Knowledge of SIEMs and ability to configure them with minimal direction, receive logs from network attached devices, and create and configure alerts for critical security events.
5. Ability to create security dashboards and reports on security status updates.
6. Skill in conducting security reviews and/or assessments of major operating systems (Microsoft, Linux, IOS), databases, web applications, and firewalls using network and web application scanning tools, scripting languages test, and report security postures/statistics.

- Ability to perform complex analyses of data and information and make recommendations.
- Ability to speak and write effectively, with emphasis on communicating technical issues to nontechnical audiences.

PREFERRED QUALIFICATIONS

- A Master's Degree in Computer Science, Computer Engineering, Information Security, or Information Assurance, or related field.
- Hands-on experience implementing and supporting at least three of the following: Cisco security devices and products, SIEMs, enterprise Endpoint security products, network and web application scanners, and Web and E-mail Security solutions.
- Experience participating in PCI-DSS and Health Insurance Portability and Accountability Act or other industry regulation audits.

EDUCATION

- A Bachelor's Degree in Computer Science, Computer Engineering, Information Security, Information Assurance, or related field, or an equivalent combination of education, experience and training that totals four years.

- A fully equivalent combination of education and training beyond what is needed to satisfy the education requirement may be used to substitute for up to two of the five years of experience. For example, a Master's Degree may be substitute for two years of experience.

CERTIFICATIONS AND LICENSES REQUIRED

- Certification as a Certified Information Systems Security Professional (CISSP) or Systems Security Certified Practitioner (SSCP) from the International Information Systems Security Certification Consortium (ICS2) or ability to obtain CISSP or SSCP certification within one year from the date of hire, promotion, or placement.

NECESSARY SPECIAL FACTORS

- Work is typically reviewed in progress and upon completion for quantity, quality, timeliness, teamwork, customer service, and other factors.
- Must be able to work varied schedule of days and outside normal business hours for scheduled and emergency maintenance and/or upgrades, as well as standard on-call rotation.
- Is subject to hold-over and recall for IT emergencies.